

Yubico Partners with OpenAI to Support Passkey Mandate for its Trusted Access for Cyber (TAC) Program Users

Passkeys anchor the transition to phishing-resistant authentication, empowering cyber defenders and Codex developers to secure the most powerful AI models and codebases.

[Yubico](#), the pioneer of phishing-resistant security keys and creator of the YubiKey, the strongest form of hardware-backed passkeys, today announced its significant role in securing the AI frontier as OpenAI mandates the use of passkeys for individuals that are part of their [Trusted Access for Cyber \(TAC\)](#) program.

As a leading global AI research and development company, OpenAI is setting a precedent for empowering its users to take control of their own security posture with more secure authentication options. Starting June 1, 2026, individuals in TAC with access to OpenAI's most powerful and permissive AI models will be required to enable [Advanced Account Security \(AAS\)](#). This mandate signals a new industry precedent: when working with agents, sensitive codebases, and powerful cybersecurity capabilities in frontier models, proven security protection like hardware-backed passkeys are no longer optional – they are the essential circuit breaker for the AI frontier.

"We are in an era where AI can analyze vulnerabilities and act on our behalf. In that world, the only thing more powerful than the AI itself is the identity of the person controlling it," said Albert Biketi, chief product and technology officer, Yubico. "OpenAI's mandate is a pivotal moment, moving the industry away from 'probabilistic' security – where we hope a password is strong enough – to a cryptographic certainty that only hardware can provide. Yubico applauds OpenAI's 'security by default' approach by enforcing rigorous security through passkeys, such as a hardware security key, for users who need it most."

Hardware-Backed AI Security Matters: How Yubico Anchors OpenAI's TAC Program

As AI evolves into autonomous agents like Codex, developer accounts become high-consequence control points. A breach now means unauthorized code access and environment manipulation. OpenAI's new mandate allows users to modernize their security posture through:

- **A Higher Level of Protection for TAC:** Utilizing passkeys, including hardware-backed passkeys like YubiKeys, provide the phishing-resistant, hardware-backed protection required for the AAS program.
- **Enterprise Attestation:** Organizations can meet OpenAI's standards by integrating Yubico's phishing-resistant authentication into their SSO workflows.
- **Zero-Knowledge Recovery:** With OpenAI removing manual account resets, Yubico's "Primary and Backup" bundles ensure users maintain mission-critical access.
- **Verifying Human Intent:** The physical "tap" of a YubiKey acts as a vital circuit breaker, ensuring high-consequence AI actions are authorized by a verified human.

This mandate builds on the Yubico and OpenAI partnership to deliver hardware-backed security to the builders of the AI future. For more information on how Yubico secures AI workflows and to access custom OpenAI YubiKey bundles, visit [Yubico's OpenAI solutions page](#).

For more information contact:

Karin Muskopf
Global Communications
press@yubico.com

About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 175 countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across more than a thousand consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA, and Singapore. For more information on Yubico, visit us at www.yubico.com.

Attachments

[Yubico Partners with OpenAI to Support Passkey Mandate for its Trusted Access for Cyber \(TAC\) Program Users](#)